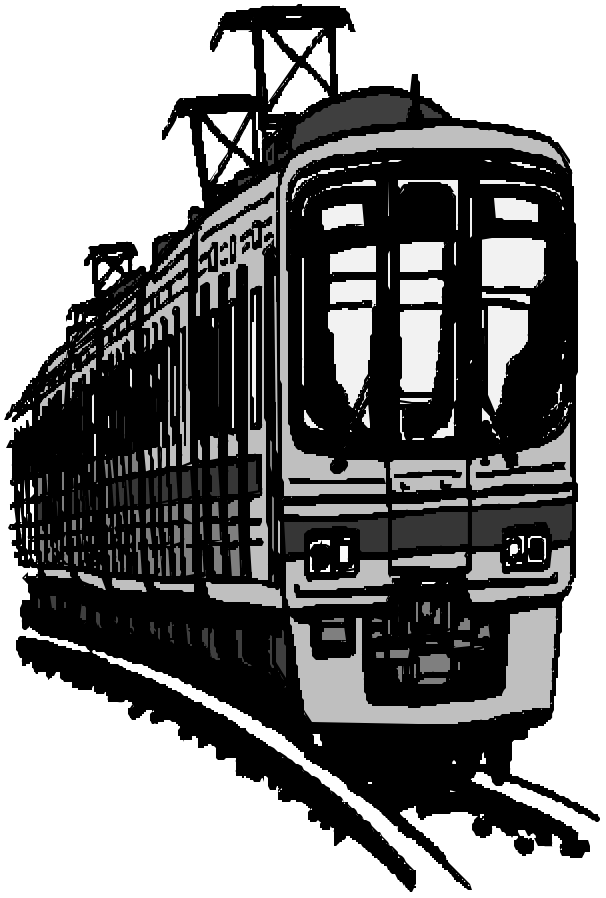
PRINCIPLES FOR A COMPREHENSIVE SECURITY STRATEGY

An Evaluation Guide for the Transportation Industry



Prepared by

STATE OF LOUISIANA
LEGISLATIVE AUDITOR

In conjunction with

Arkansas Division of Legislative Audit
Connecticut Auditors of Public Accounts
Office of the New York State Comptroller
Rhode Island Office of the Auditor General
U.S. General Accounting Office

This document is produced by the Legislative Auditor, State of Louisiana, Post Office Box 94397, Baton Rouge, Louisiana 70804-9397 in accordance with Louisiana Revised Statute 24:513. Two hundred copies of this public document were produced at an approximate cost of $624.00. This material was produced in accordance with the standards for state agencies established pursuant to R.S. 43:31. This document is available on the Legislative Auditor's Web site at www.lla.state.la.us.

In compliance with the Americans With Disabilities Act, if you need special assistance relative to this document, or any documents of the Legislative Auditor, please contact Wayne "Skip" Irwin, Director of Administration, at 225/339-3800.

OFFICE OF
LEGISLATIVE **A**UDITOR
STATE OF LOUISIANA
BATON ROUGE, LOUISIANA 70804-9397

DANIEL G. KYLE, PH.D., CPA, CFE
LEGISLATIVE AUDITOR

1600 NORTH THIRD STREET
POST OFFICE BOX 94397
TELEPHONE: (225) 339-3800
FACSIMILE: (225) 339-3870

October 21, 2002

Dear Evaluation Guide User:

This guide is the culmination of many months of collaborative work by members of my staff, participating state audit organizations, and the U.S. General Accounting Office. The fundamental purpose of this guide is to provide a framework to evaluate security efforts within our nation's transportation systems.

Since September 11, 2001, unprecedented amounts of resources have been expended on security. These expenditures may have been made without careful consideration of effectiveness and costs. As our nation continues to search for and implement new technologies and strategies to make transportation systems safer, the need for a tool to evaluate and assess security programs becomes increasingly important.

The various transportation systems in the United States are controlled by a wide variety of entities, some government and some private-sector. Railroads are mostly owned by private companies. Many highways are owned by states. However, local bus lines are usually owned by municipal governments. Thus, the security of these systems is now in the hands of thousands of different transportation system owners and operators around the country. Regardless of the organizational structure controlling a particular transportation system, the 20 principles in this guide are necessary for the development and maintenance of a comprehensive, effective, and economical transportation security strategy. The principles address the assessment of security risks, the selection of strategies or countermeasures to reduce those risks, and the preparations for responding to emergencies. The guide also contains evaluation steps that assist users in application of the principles.

Potential users of this guide include the following:

- Internal audit organizations
- External audit organizations including state, local, and federal auditors
- Transportation officials (public and private)
- Transportation security personnel (public and private)

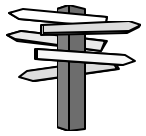
I would like to thank members of the following organizations for their hard work and effort in helping my staff to create this guide:

- Arkansas Division of Legislative Audit
- Connecticut Auditors of Public Accounts
- Office of the New York State Comptroller
- Rhode Island Office of the Auditor General
- U.S. General Accounting Office

Sincerely,

Daniel G. Kyle, CPA, CFE
Legislative Auditor

DGK:DKG:dl



CONTENTS

About the Guide

This evaluation guide was developed to assist auditors and transportation personnel in assessing the security programs for transportation assets and operations. The guide is not specific to any one mode of transportation; therefore, users may find it necessary to modify the guide to meet their specific needs.

The guide is divided into three major sections:

- Principles for Conducting a Risk Assessment
- Principles for Developing and Maintaining Countermeasures
- Principles for Emergency Preparedness

The Principles for Conducting a Risk Assessment section provides the user with a step-by-step description of the risk assessment process. The user is given the basic framework for identifying critical assets, identifying threats, and assessing vulnerability and impact.

The Principles for Developing and Maintaining Countermeasures section provides the user with a sound methodology for selecting and maintaining effective and economical security strategies.

The Principles for Emergency Preparedness section provides the user with the key elements of emergency preparedness.

In each section the principles are briefly described. A checklist is provided for each principle to help an evaluator assess the degree to which the transportation personnel are adhering to the principle. Finally, The Bottom Line is stated for each principle. This part is a series of questions that pinpoint what transportation personnel should be doing.

The guide is a valuable tool in both evaluating security strategies and strengthening strategies. The principles can serve as criteria (or standards) for the auditor to evaluate a facility's security program and as an aid to transportation management to improve its security program.

It is important to remember that products resulting from use of this guide may contain sensitive information. Every effort should be made to safeguard information regarding a facility's strengths and weaknesses.

Project Background

In March 2001, the U.S. General Accounting Office (GAO) formed a Domestic Accountability Working Group consisting of federal, state, and local government officials. This group was formed to work with GAO on issues of mutual concern. In an effort to explore opportunities for greater collaboration within the intergovernmental audit community, the group decided to develop joint projects in selected areas. The Louisiana Legislative Auditor, as a member of this group, took the lead role in the transportation area. The group decided to focus on transportation security issues.

The Louisiana Legislative Auditor then joined with the following organizations to develop this guide for transportation security:

- Arkansas Division of Legislative Audit
- Connecticut Auditors of Public Accounts
- Office of the New York State Comptroller
- Rhode Island Office of the Auditor General
- U.S. General Accounting Office

Principles for Conducting a Risk Assessment

The risk assessment process combines multiple steps to systematically produce a prioritized list of critical assets on which organizational resources can be allocated and strategies implemented.

This section contains a detailed description of the risk assessment process and the main principles involved. In our research, we identified several methods for conducting a risk assessment. In this section you will find a compilation of the essential aspects of these methods. The majority of the risk assessment methods we found involve a variation of four main steps aimed at identifying and prioritizing assets that need to be secured. These main steps are (1) identify critical assets; (2) assess threats; (3) assess vulnerability and impact; and (4) determine overall risk level.

The threat, vulnerability, and impact assessments are necessary components of a comprehensive risk assessment. Incorporation of this information allows for a thorough analysis of the transportation system and produces well-supported results. It should be emphasized, however, that a variety of models may be used to conduct the threat, vulnerability, and impact assessments. In addition, the three are not mutually exclusive. For example, one method we found does not have a separate impact assessment, but it incorporates the essential elements of an impact assessment into what it calls a vulnerability assessment. Because there is no standard model or terminology used in these methods, the order in which these operations are performed and the measures (qualitative or quantitative) used for assessment can vary from one application to another.

Rather than selecting a particular model as a standard, the principles included in this section attempt to be as inclusive as possible while retaining the essential elements of the process. For example, under the vulnerability assessment principle (principle 5), the evaluation checklist asks evaluators to determine if the factors used to rank the vulnerability of assets were relevant (i.e., related to the asset itself and its susceptibility to attack). However, the checklist does not list a specific set of factors that should be used. Because of this less restrictive format, users of this section of the guide will need to use their professional judgment when analyzing the factors used by the transportation system under review. That is, given their understanding of a vulnerability assessment, do the factors used by the transportation system under review appear relevant? Examples of factors used in the various components of the risk assessment can be found in the following sources:

- *A Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection* (AASHTO)
- *Surface Transportation Vulnerability Assessment* (U.S. DOT)
- *Fiscal Year 1999 State Domestic Preparedness Equipment Program Assessment and Strategy Development Tool Kit* (U.S. DOJ)

The process for conducting a risk assessment typically begins with a group of individuals with expertise in the transportation and security industries being assigned responsibility for planning and conducting the assessment. Their work begins with an identification of all organizational

assets. Next, those assets that are most important to the operation and security of the organization are selected for further analysis. The analysis of these critical assets involves a threat assessment to determine the likelihood of the asset coming under attack and a vulnerability assessment to determine how easily each particular asset could be successfully attacked. In addition, an impact assessment is conducted to assess the likelihood of loss of life and operational capability given that an attack is attempted. The results of the analyses are then combined to determine an overall risk level or score for each critical asset. Comparing the overall risk levels or scores from the analyzed assets enables the assessment team to rank critical assets and determine which are at greatest risk.

The risk assessment results should be reconsidered whenever there are significant changes in the transportation system or the environment in which it operates.

1. A KNOWLEDGEABLE TEAM SHOULD BE ASSIGNED THE RESPONSIBILITY OF CONDUCTING THE RISK ASSESSMENT.

A knowledgeable team of individuals who together have a comprehensive knowledge of the transportation system under review should be responsible for conducting the risk assessment. The risk assessment is largely based on the professional expertise and knowledge of those conducting the assessment. Therefore, the abilities of the team members will have a large impact on the value of the resulting assessment.

The team will be determining what assets are critical, obtaining and analyzing threat information, developing potential threat scenarios, and determining the vulnerability to and impact of specific threat scenarios on infrastructure and people. Therefore, individuals with knowledge and experience in each of these areas should participate, as appropriate, in the risk assessment.

It is not required that the team be composed of only organization staff. Some expertise can be obtained from outside the transportation organization. For example, local police and fire departments could provide information about threats and vulnerabilities.

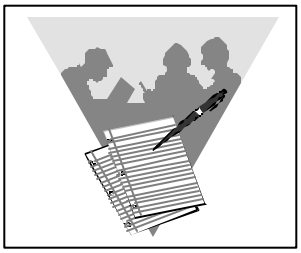
EVALUATION CHECKLIST

- ☐ Determine the process used to select team members.
- ☐ Determine if the process used to select team members is designed to select individuals with expertise in all relevant areas.
- ☐ Determine the educational and career background of the assessment team members.
- ☐ Determine if all essential roles/responsibilities have been assigned to individuals with expertise in the relevant area.
- ☐ Determine if the process used to select team members is formalized in a written policy or procedure.

THE BOTTOM LINE

- ✔ Were the assessment team members selected using a formal process based on their collective knowledge and experience?
- ✔ Is the assessment team composed of individuals who collectively have a comprehensive understanding of the transportation system under review?

2. A FORMAL AND COMPREHENSIVE ASSESSMENT PLAN SHOULD BE DEVELOPED.



There should be a formal assessment plan that outlines the scope, data requirements, methodology, schedule, logistics, and costs of the various components of a risk assessment.

The components of a risk assessment that should be included are critical asset identification, threat assessment, vulnerability assessment, impact assessment, and risk calculation.

The plan should outline the procedures to be used to oversee and conduct the various parts of the risk assessment (including the factors that will be considered when assigning risk levels or scores to assets).

The plan should also designate those responsible for ensuring that these procedures are completed in a timely manner. Top management should show its support of the risk assessment effort by approving the assessment plan.

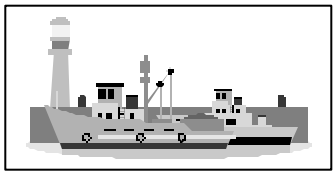
EVALUATION CHECKLIST

- ☐ Determine if the assessment plan describes the scope, data requirements, methodology, schedule, logistics, and costs for the following:
  - ✓ Critical asset identification
  - ✓ Threat assessment
  - ✓ Vulnerability assessment
  - ✓ Impact assessment
  - ✓ Risk calculation
- ☐ Determine if the lines of responsibility for conducting the various components of the risk assessment are established and documented.
- ☐ Determine if the assessment plan has been approved by top management.

THE BOTTOM LINE

- ✔ Does the facility have a comprehensive assessment plan that outlines the work to be done and includes plans for all of the essential elements of a risk assessment?
- ✔ Is the assessment plan reviewed regularly, revised as needed, and approved by top management?

3. CRITICAL ASSETS SHOULD BE IDENTIFIED AND DOCUMENTED USING A SYSTEMATIC METHOD.



Assets may include facilities, vehicles, equipment, people, information, and activities/ operations. Critical assets are defined as those assets that are essential to the transportation system's ability to provide service and to maintain safety.

Critical assets should be selected from a list of all assets. This process promotes efficiency as it reduces the number of assets that must undergo additional analyses. When determining which assets are critical, the team should consider the value of each asset to the organization's operations and safety.

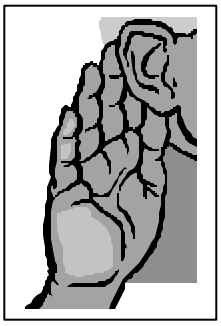
EVALUATION CHECKLIST

- ☐ Determine the method used to identify critical assets.
- ☐ Determine if the method used included all assets.
- ☐ Determine if the method considered the impact on people (service, safety).
- ☐ Determine if the method considered the impact on the operations of the transportation system.
- ☐ Determine if the method was consistently applied to each asset.
- ☐ Determine if the method used ranked the assets based on criticality.
- ☐ Determine if the information outlining the criticality of each asset was documented.
- ☐ Determine if the assessment team followed the methodology for identifying and documenting critical organizational assets as specified in the assessment plan.

THE BOTTOM LINE

- ✔ Did the assessment team systematically identify and assess the criticality of the assets?
- ✔ Was the method used to assess the criticality of organizational assets reasonable?
- ✔ Were the method and results of the criticality assessment documented?

4. CREDIBLE THREAT INFORMATION SHOULD BE ACTIVELY PURSUED.



Threats are expressions of intent to cause injury or death to people or damage to critical assets. The assessment team should identify threats through information obtained from federal, state, or local government, private/non-government organizations, similar entities, historical data, local crime patterns, etc. If possible, intelligence information should be obtained and analyzed based on the likelihood of the threat becoming a reality. Relevant criteria (or standards) should be used to analyze threat information (e.g., existence of a group who wants to attack the organization, the capabilities of the group). At a minimum, the assessment team should identify potential threats and develop threat scenarios to use in the risk assessment.

The assessment team should ensure that the identified threats are incorporated into the overall risk assessment results.

EVALUATION CHECKLIST

- ☐ Determine what method(s) were followed to obtain threat information.
- ☐ Determine if any obstacles were encountered in collecting intelligence information. If so, determine what alternative methods were developed for gathering threat information.
- ☐ Determine if the threats were analyzed using relevant criteria (or standards).
- ☐ Determine if the threat analysis criteria were consistently applied.
- ☐ Determine if the threat information was incorporated into overall risk assessment results.
- ☐ Determine if the team documented sources of information.
- ☐ Determine if the team followed the threat assessment methodology specified in the assessment plan.

THE BOTTOM LINE

- ✔ Did the assessment team actively seek threat information from reliable sources?
- ✔ Did the team identify and analyze threat information using reasonable, logical, and consistent methods?
- ✔ Are threats well documented and incorporated into the overall risk assessment results?

5. THE VULNERABILITY OF CRITICAL ASSETS SHOULD BE SYSTEMATICALLY ANALYZED.

Vulnerabilities are physical, technical, administrative, procedural, or human-related characteristics of an asset that make it susceptible to breaches in security (e.g., accessibility of the asset or the presence of hazardous materials at the asset site). The vulnerability assessment is designed to systematically measure the susceptibility of critical assets to hazards. This assessment should highlight system weaknesses that can be exploited.

The team may use potential threats to assess the vulnerability of each critical asset. In assessing asset vulnerability, the assessment team should (1) develop a group of factors that will be used to judge the vulnerability of each critical asset; (2) assess each asset using the factors developed; (3) use a systematic process to rank the vulnerability of each critical asset; and (4) ensure the results of the vulnerability assessment are incorporated into the overall risk assessment results.

EVALUATION CHECKLIST

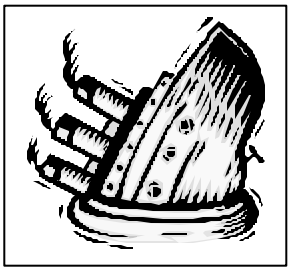
- ☐ Determine the method used to conduct the vulnerability assessment.
- ☐ Determine if factors used to rank the vulnerability of assets in the assessment were relevant (i.e., related to the asset itself and its susceptibility to attack).
- ☐ Determine if the factors were consistently applied to each asset.
- ☐ Determine if a systematic process was used to assess and rank the vulnerability of each critical asset.
- ☐ Determine if the results of the vulnerability assessment were incorporated into the overall risk assessment results.
- ☐ Determine if the team followed the vulnerability assessment methodology specified in the assessment plan.

THE BOTTOM LINE

- ✔ Was a systematic vulnerability assessment conducted for all critical assets?
- ✔ Were the results of the vulnerability assessment incorporated into the overall risk assessment results?
- ✔ Did the team conduct a systematic vulnerability assessment on all critical assets using reasonable, logical, and consistent methods?

6. A SYSTEMATIC METHOD SHOULD BE USED TO ESTIMATE THE IMPACT OF AN ATTACK ON CRITICAL ASSETS.

When conducting an impact assessment, the team should consider human and economic loss factors. Human loss can be calculated in terms of fatalities and injuries. Economic loss involves the direct costs of destroyed property, repair, and cleanup costs, as well as the costs of the disruptions in service (including contingency plans).



The team should use a systematic method to determine the impact of an incident involving each critical asset. The factors used to assess impact should be applied consistently and documented. There should be a systematic process for ranking the impact on each critical asset. The team should ensure that the results of the impact assessment are incorporated into the overall risk assessment results.

EVALUATION CHECKLIST

- ☐ Determine the methodology used to conduct the impact assessment.
- ☐ Determine if the factors used in the assessment were relevant (i.e., related to human and economic losses) and included contingency plans and the cost of such plans.
- ☐ Determine if the factors were consistently applied to all critical assets.
- ☐ Determine if the impact assessment process provided a method to rank the assets based on the impact.
- ☐ Determine if results of the impact assessment were incorporated into the overall risk assessment results.
- ☐ Determine if the team followed the impact assessment methodology specified in the assessment plan.

THE BOTTOM LINE

- ✔ Was a systematic method used to assess and rank the impact of an attack on critical assets?
- ✔ Were factors used in the impact assessment relevant and consistently applied?
- ✔ Were the results of the impact assessment incorporated into the overall risk assessment results?
- ✔ Did the team conduct a systematic impact assessment on all critical assets using reasonable, logical, and consistent methods?

7. A SYSTEMATIC METHOD SHOULD BE USED TO ASSESS THE OVERALL RISK LEVEL OF CRITICAL ASSETS.

The overall risk assessment results should be a combination of the (a) threat assessment (principle 4), (b) vulnerability assessment (principle 5), and (c) impact assessment (principle 6). There are a variety of models that may be used to determine the overall risk level. These different models perform the three assessments in different orders and in some cases combine assessments. Regardless of which method is used, all three assessments should be included.

The risk assessment results will reveal which critical assets are at highest risk for a security breach. The results will also help the team to determine where resources should be allocated.

EVALUATION CHECKLIST

- ☐ Determine if a systematic method was used to attain the overall risk assessment results.
- ☐ Determine if the methodology used incorporated information from the threat, vulnerability, and impact assessments.
- ☐ Determine if the team properly documented the methodology and results of the overall risk assessment results.

THE BOTTOM LINE

- ✔ Did the team incorporate information from the threat, vulnerability, and impact assessments and determine the overall risk level of each critical asset using reasonable, logical, and consistent methods?
- ✔ Were the methodology and results of the risk assessment properly documented?

8. RISKS SHOULD BE REASSESSED WHENEVER THERE ARE SIGNIFICANT CHANGES TO THE TRANSPORTATION SYSTEM OR ITS ENVIRONMENT.

New facilities or changes in the organization's operations or mission may change the list of assets considered critical. Similarly, significant structural modifications may affect existing vulnerability and impact assessments. In addition, new information about credible threats to an organization's assets (including the occurrence of actual incidents) would make prior threat assessments obsolete. Therefore, when these types of events occur, the risk assessment results should be reevaluated.

EVALUATION CHECKLIST

- ☐ Determine if a mechanism is in place to trigger a revision of the current risk assessment results.
- ☐ Determine if this mechanism incorporates possible changes to each component of the risk assessment (critical asset identification, threat, vulnerability, and impact assessments).
- ☐ Determine if this mechanism causes a reassessment if significant changes take place to the transportation system or the environment in which it operates.

THE BOTTOM LINE

- ✔ Is there a mechanism in place to monitor for significant changes to the criticality of assets and the nature of threats, vulnerabilities, and impacts?
- ✔ Are risks reassessed whenever there are significant changes to the transportation system or its environment?

Principles for Developing and Maintaining Countermeasures

After a comprehensive risk assessment has been completed, facility management should begin the process of selecting countermeasures. Countermeasures are actions and devices used to prevent or counteract a security threat (e.g., perimeter fencing, cameras, or safety training). The selection of countermeasures can be challenging because it involves careful allocation of what are often scarce resources.

In selecting countermeasures, facility management must make decisions based on the following:

- Effectiveness of proposed countermeasures
- Estimated cost of proposed countermeasures
- Reduction of risks

Once countermeasures are in place, facility management must develop a means by which those countermeasures are evaluated for performance and effectiveness.

The following principles offer guidance to facilities in selecting and maintaining the appropriate countermeasures. By using these principles, facility management can be assured that it has followed a sound course in selecting and employing the most effective and economical countermeasures.

9. COUNTERMEASURES SHOULD BE SELECTED USING A SYSTEMATIC PROCESS THAT IS DRIVEN BY THE RESULTS OF A RISK ASSESSMENT.

Countermeasures should reduce the potential for or consequences of an incident based on the specific threats and vulnerabilities identified during a risk assessment.

In selecting countermeasures, facility management must carefully weigh effectiveness and cost in an organized, systematic process. Effectiveness should be determined by how well the countermeasure can reduce the occurrence or ill effects of threats and vulnerabilities that were identified during the risk assessment. Cost estimates should consider the acquisition, operation, and maintenance of countermeasures as well as added demands on staff and time.

EVALUATION CHECKLIST

- ☐ Determine how countermeasures are selected. What process is used?
- ☐ Determine if risk assessment results were used in selecting countermeasures.
- ☐ Determine if selected countermeasures lower the highest risks as identified by the risk assessment.
- ☐ Determine if the selection process allows for comparison of proposed counter-measures based on effectiveness and cost.
- ☐ Determine if the selection process is being applied consistently to all countermeasures considered.
- ☐ Determine if a written selection process exists and if it is being followed.

THE BOTTOM LINE

- ✔ Do countermeasures reduce the highest risks that were identified during the risk assessment?
- ✔ Were cost and effectiveness of countermeasures considered in their selection?
- ✔ Were countermeasures selected in an organized and consistent process?
- ✔ Did the team select countermeasures using reasonable, logical, and consistent methods that include consideration of effectiveness, cost, and results of risk assessment?

10. THE PERFORMANCE AND COST OF COUNTERMEASURES SHOULD BE TRACKED.

Facility management should develop objective methods to track the performance of countermeasures.

Performance indicators that measure outcomes are especially useful, such as number of thefts or level of customer confidence. However, measuring outcomes may be difficult because of the preventive nature of countermeasures and the infrequency of some types of security threats, such as terrorism. In these cases, changes in the amount of criminal activity can be used to gauge performance. Facilities may also use mock/test exercises to measure the effectiveness of countermeasures over time.

Measuring outcomes can also be difficult when a countermeasure is implemented in phases or over a long period of time. In these instances, it may be appropriate to measure intermediate outcomes or outputs that show progress until the countermeasure is fully implemented.

In addition to tracking performance, facility management should track the cost of countermeasures. By doing so, comparisons of effectiveness and cost can be made more easily.

EVALUATION CHECKLIST

- ☐ Determine if relevant performance indicators are being used to track countermeasures.
- ☐ Determine if performance indicators measure outcomes (results) or intermediate outcomes if appropriate.
- ☐ Determine if controls are in place to ensure the accurate collection and tallying of performance data.
- ☐ Determine if a process exists to track the cost of countermeasures.
- ☐ Determine if controls are in place to ensure that cost-tracking data are accurate.

THE BOTTOM LINE

- ✔ Does management use relevant and reliable outcome-based performance indicators to track the effectiveness of countermeasures?
- ✔ Does management use a reliable method to track the cost of countermeasures?

11. COUNTERMEASURES SHOULD BE REVIEWED ON A REGULAR BASIS.

A process should exist for facility management to periodically review existing countermeasures to ensure that they remain effective and economical.

The process should involve feedback on implementation, review of performance data and cost data, and use of the latest risk assessment results.

In addition, the process should allow for consideration and adoption of new and improved countermeasures as well as the elimination of ineffective countermeasures. The adoption and elimination of countermeasures should be based on their ability to reduce risks and should undergo the countermeasure selection process. (See principle 9.)

EVALUATION CHECKLIST

- ☐ Determine if the facility reexamines countermeasures on a regular basis.
- ☐ Determine how performance data and cost data are used in reexamining countermeasures.
- ☐ Determine if the review of countermeasures includes use of the latest risk assessment results.
- ☐ Determine how ideas for new and improved countermeasures are proposed.
- ☐ Determine if new countermeasures are chosen and existing countermeasures eliminated using a systematic selection process that considers cost and effectiveness.
- ☐ Determine if there are written procedures for the periodic review of countermeasures and determine if these procedures are followed.

THE BOTTOM LINE

- ✔ Does the facility have a reasonable, logical, and consistent process (that includes review of performance data, cost data, and updated risk assessment results) to ensure that existing countermeasures remain cost-effective?
- ✔ Does a process exist that allows for the consideration and adoption of new countermeasures and the elimination of ineffective countermeasures?

12. COUNTERMEASURES SHOULD BE RESPONSIVE TO THREAT LEVELS.

A threat level system provides a set of warnings that graduate as the level of threat increases. Facility management should adopt a threat level system that will provide the basis to adjust the intensity and amount of security. This practice will promote conservation of resources because the use of countermeasures will correspond directly with security needs.

A facility's threat level system should be compatible with a nationally or statewide recognized system. This system would allow a facility to minimize the possibility of error and confusion during times of emergency.

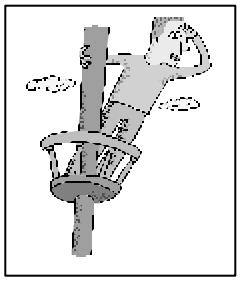
EVALUATION CHECKLIST

- ☐ Determine if the facility has a threat level system.
- ☐ Determine if the facility's threat level system is compatible with a nationally or statewide recognized system.
- ☐ Determine if written directives or procedures exist that allow counter-measures to be adjusted based on threat level.

THE BOTTOM LINE

- ✔ Does the facility adjust its use of countermeasures based on threat levels?
- ✔ Is the facility's threat level system compatible with a generally recognized federal or state system?

13. AWARENESS TRAINING SHOULD BE INCLUDED IN A FACILITY'S SECURITY EFFORTS.



Employees, vendors, contractors, and any persons with a stake in the transportation facility should be trained to identify and report suspicious activity. Awareness training can include instruction on being aware of one's physical environment, briefings on current threats, information on how to identify suspicious behaviors, and proper procedures for reporting. Awareness training should be incorporated into a facility's existing training and be provided on a regular basis.

A facility can also benefit from making its passengers more aware. Passengers can be encouraged to identify and report suspicious activities or packages. Facility management can reach and inform passengers through the use of posted notices, information pamphlets, and public announcements.

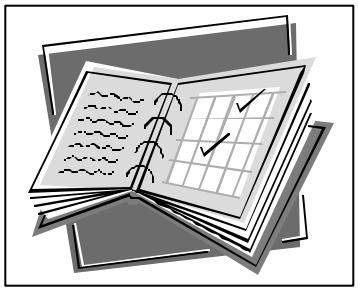
EVALUATION CHECKLIST

- ☐ Determine if the facility offers awareness training.
- ☐ Determine the purpose of the training.
- ☐ Determine if the training targets all stakeholders.
- ☐ Determine if the training is provided on a regular basis.

THE BOTTOM LINE

- ✔ Does the facility offer ongoing awareness training to educate stakeholders in identifying and reporting suspicious activities?

14. COUNTERMEASURES SHOULD BE INTEGRATED INTO SECURITY OPERATIONAL PLANS.



Facility management should develop a security operational plan that provides for day-to-day security activities. All security countermeasures should be included in the operational plan along with procedures for implementation.

Precautions should be taken to control the distribution and availability of the security operational plan.

EVALUATION CHECKLIST

- ☐ Determine if the facility has a security operational plan or a document that outlines daily security operations.
- ☐ Determine if the security operational plan includes implementation procedures for all applicable countermeasures.
- ☐ Determine when the plan was developed.
- ☐ Determine how often the plan is updated.
- ☐ Determine what measures are in place to control the plan's distribution and availability.
- ☐ Determine if the procedures for countermeasures that are outlined in the plan are actually implemented.

THE BOTTOM LINE

- ✔ Does the facility have an updated, current security operational plan that outlines daily security efforts and includes procedures for implementing countermeasures?
- ✔ Does the facility implement all countermeasures as outlined in the security operational plan?
- ✔ Are reasonable controls in place to check the availability and distribution of the security operational plan?

15. THE FACILITY SHOULD HOST REGULARLY SCHEDULED SECURITY MEETINGS.

Facility management should host regularly scheduled security meetings. Participants should include security personnel from the facility along with representatives from entities that have an interest in the facility's protection. Depending upon the mode of transportation, the following representatives should be in attendance:

- Local, state, and federal regulatory agencies
- Local, state, and federal law enforcement agencies
- Emergency responders (fire, EMS, hospital)
- Private operators within the facility (vendors, contractors)

It may also be useful to encourage participation from peer transportation facilities in the surrounding area.

These meetings should cover a variety of subjects and serve as forums for disseminating threat information, sharing new ideas and strategies, and distributing emergency preparedness and response information.

EVALUATION CHECKLIST

- ☐ Determine if the facility hosts meetings between its security personnel and groups having an interest in the facility's protection.
- ☐ Determine how often meetings are held.
- ☐ Determine who is in attendance at the meetings.
- ☐ Determine what is included on meeting agendas.

THE BOTTOM LINE

- ✔ Does the facility host regularly scheduled security meetings between its security personnel and representatives from groups having an interest in the facility's protection?

Principles for Emergency Preparedness

It is important that an organization be well prepared to respond to an emergency. Emergency response procedures should be developed and validated before an incident occurs. The transportation entity may have its own emergency response plan or may be a part of a larger plan. In either case, the response to an emergency at a transportation facility will usually include several outside entities (e.g., local police and fire departments). The organization should coordinate its procedures with local emergency response management agencies to ensure an efficient and effective response plan.

A qualified team of individuals should develop a comprehensive emergency response plan. Federal (and possible state) regulations exist for emergency planning. Therefore, the planning team must ensure compliance with applicable regulatory requirements.

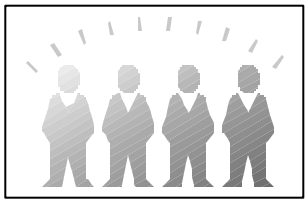
If an organization has an existing all-hazards emergency response plan, it should be revised to incorporate procedures specific to a terrorist attack. The literature reviewed revealed the principles in this section as the key elements of emergency preparedness.

.

16. A qualified team of individuals should be formed to create an emergency response plan.

The team should consist of representatives from the transportation system and, depending upon the mode of transportation, representatives from the following entities:

- Local, state, and/or federal law enforcement agencies
- Local, state, and/or federal regulatory agencies
- Area fire department
- Emergency medical service
- Local and/or state office of emergency preparedness



A team approach is recommended because it (1) inspires buy-in from the participating entities; (2) allows more knowledge and expertise to shape the planning process; and (3) creates closer professional relationships among those involved, thereby encouraging coordination and teamwork.

EVALUATION CHECKLIST

- ☐ Determine if the facility has an emergency response plan.
- ☐ Determine what entities are represented by the team that created the plan.
- ☐ Determine if all entities that are responsible for emergency response are represented on the team.
- ☐ Determine if team members possess knowledge of emergency response planning.

THE BOTTOM LINE

- ✔ Did a qualified team of representatives from all entities responsible for responding to an emergency develop an emergency response plan for the facility?

17. The emergency response plan should be comprehensive and in compliance with all regulatory requirements.

The following components are essential to a complete emergency response plan:

- Procedures for notification and activation of crisis management teams
- Procedures for evaluating threats and categorizing them within a predetermined security level system
- Identification of roles/responsibilities of players
- Identification of evacuation procedures
- Procedures for dealing with victims' families
- Procedures for coordination with local emergency responders
- Procedures to ensure the safety and security of residents after the initial incident
- Procedures to issue public information through the media
- Procedures to restore service or create service alternatives
- Revision of all-hazard plan to include terrorism

The team should ensure the emergency response plan conforms to applicable regulatory requirements and the standards of federal, state, local, and/or oversight agencies.

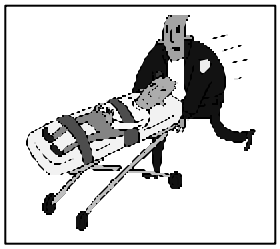
EVALUATION CHECKLIST

- ☐ Determine if the emergency response plan includes all essential components.
- ☐ Determine if procedures are in place to ensure that the emergency response plan conforms to all regulatory requirements.

THE BOTTOM LINE

- ✔ Is the emergency response plan comprehensive and in compliance with regulatory requirements?

18. The emergency response plan should be practiced regularly.



Training exercises should be conducted regularly with all those involved in the response effort. Training may include tabletop exercises, regular drills, surprise drills, and full-scale simulations. These exercises identify potential problems with the response plan and ensure readiness.

EVALUATION CHECKLIST

- ☐ Determine if the emergency response plan is regularly practiced.
- ☐ Determine when the latest practice exercises occurred.
- ☐ Determine if emergency response personnel found the training exercises to be useful.

THE BOTTOM LINE

- ✔ Is the emergency response plan practiced on a regular basis and are practice exercises useful?

19. The emergency response plan should be reviewed and updated regularly and after each use.

The plan should be modified in response to continually changing security threats in order to remain useful and up-to-date. Reviews should be conducted on an annual basis at a minimum.

Information learned from training exercises and actual incidents should be incorporated into future response plans.

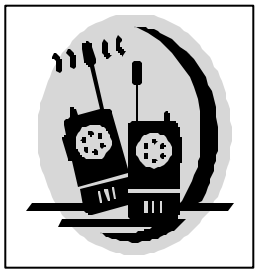
EVALUATION CHECKLIST

- ☐ Determine if the emergency response plan is regularly reviewed and updated.
- ☐ Determine when the latest review and revisions occurred.
- ☐ Determine if procedures are in place to incorporate the results of training exercises and actual incidents into emergency response plans.

THE BOTTOM LINE

- ✔ Is the emergency response plan updated and revised regularly?
- ✔ Are the results of training exercises and actual incidents incorporated into future emergency response plans?

20. A multi-modal communications system should be established.



Radio communications systems should be established for use in emergency situations. These systems should use technologies that permit transportation personnel, crisis management teams, and emergency responders (e.g., EMT, fire, police) to exchange information in a timely manner and conduct an efficient response effort.

A backup communication system should be established in preparation for failure of the primary system. There should be a mechanism for notifying all individuals involved in the response effort when a switch to the backup is to take place.

EVALUATION CHECKLIST

- ☐ Determine if common communication exists between emergency response personnel.
- ☐ Determine if a backup communication plan exists.
- ☐ Determine how well the system functions.
- ☐ Determine how often the system is checked for proper operation.

THE BOTTOM LINE

✔ Are emergency response personnel able to communicate effectively with each other?

Source List

American Association of Railroads (AAR): *Terrorism Risk Analysis and Security Management Plan*

American Association of State Highway and Transportation Officials (AASHTO): *A Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection*

Critical Infrastructure Assurance Office (CIAO): *Practices for Securing Critical Information Assets*

Federal Emergency Management Agency (FEMA): *Guide for All-Hazard Emergency Operations Planning*

Federal Transit Authority (FTA): "Security Round Table: Incorporating Security into the Oversight Program"

Florida Statute 311.12, "Seaport Security Standards and Compliance Plan"

Haimes, Yacov, "Virginia's Critical Infrastructure Protection"

Interagency Commission on Crime and Security in U.S. Seaports: *Report of the Interagency Commission. . .*

Mineta International Institute for Surface Transportation Policy Studies: *Protecting Surface Transportation Systems and Patrons from Terrorist Activities*

Mineta Transportation Institute (MTI): *Protecting Public Surface Transportation Against Terrorism and Serious Crime: An Executive Overview*

Office of Homeland Security: *Securing the Homeland, Strengthening the Nation*

U.S. Department of Transportation (U.S. DOT): *Surface Transportation Vulnerability Assessment*

U.S. Department of Justice (U.S. DOJ): *Fiscal Year 1999 State Domestic Preparedness Equipment Program Assessment and Strategy Development Tool Kit*

U.S. General Accounting Office (GAO): *Combating Terrorism: Critical Components of a National Strategy to Enhance State and Local Preparedness*